PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Financial Services Center (FSC)
Financial Healthcare Services (FHS)

Fraud Waste and Abuse Software

Date:
PWS Version Number: 1.0

CONTENTS

1.0 PURPOSE

The purpose of this requirement is to acquire a Fraud, Waste and Abuse (FWA) Prevention System and associated operational services to support the workload of the Department of Veterans Affairs (VA), Financial Services Center (FSC). The Contractor, acting independently and not as an agent of the government, shall furnish all the necessary services, qualified personnel, material, equipment, supplies, and facilities except as otherwise specified herein, and otherwise do all things necessary for or incident to performance of requirements described in this work statement, also referred to as the Contractor's Statement of Work (SOW).

2.0 BACKGROUND

The Department of Veterans Affairs (VA), Financial Services Center (FSC) is authorized by the Government Management Reform Act of 1994 (Public Law 103-356) to provide common administrative support services on a reimbursable basis to VA and Other Government Agencies (OGA's), as a Franchise Fund. The goals of the Franchise Fund organizations include:

Lowering overhead costs
Improving the quality and delivery of services
Creating economies of scale
Eliminating redundant services
Being auditable

The purpose of this procurement is to procure commercial-off-the-shelf (COTS) software designed to detect Fraud, Waste and Abuse (FWA) and associated operational services to support the workload. FSC requires this software to detect FWA from the healthcare claims that are submitted by healthcare providers. This COTS configurable software will serve with the VA-FSC's healthcare claims adjudication enterprise solution, eCAMS HCE. The Contractor, acting independently and not as an agent of the government, shall furnish all the necessary services, qualified personnel, material, equipment, supplies, and facilities except as otherwise specified herein, and otherwise do all things necessary for or incident to performance of requirements described in this work statement, also referred to as the Contractor's Performance Work Statement (PWS).

The intent of the software is to eliminate false claims. The False Claims Act (31 U.S.C. §3729), allows American citizens, whether affiliated with the government or not, to file actions against federal contractors claiming fraud against the government.

The False Claims Act was passed by Congress to prevent the United States Government from paying federal funds for fraudulent claims involving goods and services. For VA, this would include submitting false information in order to receive a higher reimbursement. Examples of this include upcoding (i.e., coding a higher DRG than the documentation support), lab unbundling (i.e., charging separately for procedures usually charged as one procedure), billing for services not actually rendered and duplicative billing.

The False Claims Act outlines the federal penalties for submitting false claims, as well as protections granted to an individual who reports a violation.

VA-FSC is measured on Return on Investment "ROI" of the FWA program. To improve the long term ROI and align with FSC's organizational goal, FWA software is being undertaken to enable more efficient processing. By investing in a FWA system, VA- FSC expects a range of benefits, including cost savings in operational IT infrastructures, improved cost recovery from administrative actions, improved prevention and detection of fraud, waste and abuse in the claims processing spending.

VA-FSC requires a system that can be used to provide analytics that identified billing pattern that might indicate potential fraud, waste and abuse. Increased healthcare demands require organizations who adjudicate healthcare claims to modernize their core administrative systems to be more efficient. As a franchise organization, the FSC has existing and potential customers that can be migrated into the system.

VA-FSC has adopted eCAMS HCE software to adjudicate, process, and pay healthcare claims. The Contractor shall enhance the system to meet evolving VA-FSC FWA business requirements and support migration to the new healthcare claims adjudication enterprise solution eCAMS HCE.

After software has been procured; configurations have been made, business rules have been incorporated, and the resulting software has been integrated with existing support systems and put into production; the FWA system will allow for real time FWA detection within claims adjudication process before payment of the claim.

Notice of OI&T Migration from PMAS to VIP: OI&T intends to transition projects from the PMAS project management process into the Veteran-focused Integration Process (VIP) project management process in the 2016-2017 timeframe (https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371). The Veteran-focused Integration Process (VIP) is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise.

VIP is the follow-on framework from Project Management Accountability System (PMAS) for the development and management of IT projects which will propel the Department with even more rigor toward Veteran-focused delivery of IT capabilities. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence.

VIP is a significant evolution from PMAS, creating a more flexible process that has fewer documentation requirements and milestones, and delivers products in shorter increments. VIP is

currently undergoing a Pilot Program and is currently in a draft state and will continue to evolve. Once the pilot is complete, requirements outlined in this PWS may be transitioned to the VIP framework during the Period of Performance of this contract.

3.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
6. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
7. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, http://www.va.gov/vapubs/
8. VA Handbook 0710, Personnel Suitability and Security Program, May 2, 2016, http://www.va.gov/vapubs
9. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
10. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
11. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
12. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
14. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
15. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
16. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
17. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
18. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
19. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", July 28, 2016
20. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
21. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010
22. VA Handbook 6500.6, "Contract Security," March 12, 2010

23. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
24. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
25. OI&T ProPath Process Methodology (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp
26. One-VA Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, VA Privacy Impact Assessment, October 15, 2014
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, "Transition to IPv6", September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015.
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014
34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
35. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
36. OMB memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
43. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)

46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
49. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
51. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
54. Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," October 5, 2009
55. Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," January 24, 2007
56. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
57. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
58. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
59. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
60. VA Directive 6071, Project Management Accountability System (PMAS), February 20, 2013
61. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
62. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
63. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

4.0 SCOPE

The Contractor shall provide VA-FSC with Fraud, Waste and Abuse software that meets the VA-FSC requirements identified in this PWS. The Contractor shall provide a perpetual license allowing unlimited use of the software product in perpetuity; as well as configuration, implementation, integration, testing, deployment of software, training, maintenance, and technical support. The Contractor shall follow an Agile Methodology and follow VIP established by OI&T Enterprise Program Management Office (EPMO). The Contractor shall also provide quality improvement services (see Section 7.0) throughout the duration of the contract.

5.0 PERFORMANCE DETAILS

5.1 PERFORMANCE PERIOD

The period of performance (POP) shall consist of one initial period of 12 months from date of award, followed by three (3) option periods of 12 months each.

When work is performed at a VA facility; contract personnel shall maintain a work schedule that coincides with the schedule of the VA-FSC organizations they support. Normal Federal Government workdays are between core hours of 0600 (6:00 AM) Central Time (CT) and 1800 (6:00 PM) CT.

On occasion, Contractor personnel may be required to provide services outside of normal hours of duty. When this happens, Contractor personnel shall comply with the VA-FSC's requirements. Contractor personnel shall not work during off-duty hours unless authorized in advance by the Contracting Officer's Representative (COR). The COR and the Contractor shall mutually agree upon all deviations to the schedule.

Any work at a Government site shall not take place on Federal holidays or weekends, unless directed by the Contracting Officer (CO). If required, the CO may require to work during holidays and/or weekends. At a minimum, at least one Federal Government employee whose duties are relevant to the scope of this PWS must be present whenever Contract personnel perform work defined in this PWS at a VA facility.

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving Fourth	Thursday in November

5.2 PLACE OF PERFORMANCE

Software procured under this contract shall be installed in the VA-FSC facility in Austin, Texas; but will need to undergo configuration, implementation, integration, and testing to ensure it meets VA-FSC requirements, before it can be deployed into production. Initial configuration, implementation, testing, and integration will be performed by the Contractor at their facility, prior to the software being delivered to VA-FSC. Once delivered, the Contractor shall install and further configure, test, and implement the software at the FSC facility to ensure its ability to be deployed into production. Subsequent configuration, integration, testing, and implementation will be performed by the Contractor and VA-FSC technical resources throughout the life of the contract. This work will take place at both the Contractor's facility and the FSC government facility, as directed by FSC program management staff.

5.3 TRAVEL

Costs for all travel associated with the tasks specified in section 6 of this PWS shall be borne by the contractor and shall not be separately reimbursed by the government.

6.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

6.1 PROJECT MANAGEMENT

6.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor’s approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the tasks, sub-tasks, schedule and timelines, milestones, resource support, and risks. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance. The schedule and timelines shall be segregated by period, i.e. one initial two-year period plus each of three option periods, such that there is no overlap in periods for any scheduled activity, i.e. successful completion of work identified under any one period is not contingent on the exercise of any option period. The Contractor shall plan for 90-day period for VA testing to support production release and “go

live" for each program offering. The Contractor shall update and maintain the VA Program Management approved CPMP, and submit the updated plan monthly, throughout the period of performance. The contractor shall submit the initial CPMP no later than 2 business days prior to the PAOC.

The monthly update to the CPMP shall cover all work completed during the month preceding the month during which the update is delivered, plus work planned for the month in which the update is delivered and any subsequent period within six months of the date of delivery. The update shall also identify any problems that arose and either a description of how the problems were resolved, or suggested resolutions, if problems were not resolved during the reporting period. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving each issue. The update shall also include any change in Contractor staff involved in the work identified in this PWS. The Contractor shall monitor performance against the CPMP and report any deviations. The Contractor is required to communicate problems and issues to the VA within three calendar days of discovery, to ensure issues identified on the report are transparent to both parties and to prevent escalation of outstanding issues

Deliverable:

A. Contractor Project Management Plan

6.1.2 POST AWARD ORIENTATION CONFERENCE (PAOC)

The Contractor shall participate (in person or virtual) in the PAOC at the VA-FSC in Austin, TX within seven calendar days after contract award, and cover the following information during the PAOC:

a. Details regarding Tasks, Subtasks, Timelines, and the Delivery Schedule for the Project Plan
b. Names and credentials for all Contractor resources who will participate in contract implementation (by Contractor)
c. Schedule for meetings with FSC Team members, Government counterparts to Contractor staff, Contractor staff, and Data Contacts resources.

The Contractor shall document the PAOC meeting minutes detailing what was discussed, list of attendees, expectations of Contractor, expectations of VA-FSC, and any actions required of each party.

Deliverable:

A. PAOC Meeting Minutes

6.1.3 REPORTING REQUIREMENTS

The Contractor shall provide the COR with Monthly Progress Reports in electronic format, in Microsoft Word. The report shall include detailed explanations for each required data element, to ensure that data is accurate and consistent. This report shall reflect data through the last day of the preceding month.

The Monthly Progress Report shall cover all work completed during the month preceding the month during which the report is delivered, plus work planned for the month in which the report is delivered and any subsequent period within six months of the date of delivery. The report shall also identify any problems that arose and either a description of how the problems were resolved, or suggested resolutions, if problems were not resolved during the reporting period. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving each issue. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables and their current Section 508 conformance status. The report shall also include any change in Contractor staff involved in the work identified in this PWS. The Contractor shall monitor performance against the CPMP and report any deviations. The Contractor is required to communicate problems and issues to the VA within three calendar days of discovery, to ensure issues identified on the report are transparent to both parties and to prevent escalation of outstanding issues

Deliverable:

A. Monthly Progress Report

6.2 SOFTWARE PRODUCT/LICENSE

The Contractor shall have the option to propose a perpetual license for FWA software native to the FSC healthcare claims adjudication enterprise solution eCAMS HCE or as a stand-alone solution. The FSC currently services a number of customers and as a Franchise organization; they have the ability to service additional customers with our healthcare claim processing product line. In order to enable and provide expansion capability, the software shall be capable of scaling to an estimated annual volume of 30 million claims. As the FSC's customer base expands, the software will need to continue to scale to meet the performance requirements outlined in section 6.3. The Contractor shall also scale the corresponding support required by PWS sections 6.3.8.

Deliverables:

A. Software Product/License

6.2.1 PERPETUAL SOFTWARE PRODUCT/LICENSE

The Contractor shall provide the FWA software product meeting the requirements specified below in section 6.2 and its subparagraphs and allow VA-FSC unlimited use of the software product in perpetuity. The Government shall retain unlimited data rights for any software developed to meet the requirements of this contract.

6.3 SYSTEM FEATURES AND CAPABILITIES

The FWA system will serve with the VA-FSC's healthcare claims adjudication enterprise solution eCAMS HCE, and provide real-time pre-payment fraud detection.

Where the requirements call for integration to an existing VA system, the FSC will be responsible for the execution of the interface between the vendor's COTS software and existing SOA interfaces.

6.3.1 LANDING PAGE INTERFACE

a. Provides system status messages (planned system outages and system messages)
b. Displays individual user information (user name, role, user ID, user organization and last login date/time, claims in que, claims last processed)
c. Displays role-based Alert Summary Reporting (ASR) and Case Management Dashboard link
d. Displays role-based Business Intelligence Reporting link
e. Displays Claim Query, Search and Export Reporting link
f. Displays Informational Quick link (production issues, training schedule, model information guide and user manual)
g. Displays Help Desk (IT Service Desk) providing phone number and email.

6.3.2 PREDICTIVE ANALYTICS-BASED FRAUD, WASTE AND ABUSE (FWA) DETECTION

a. Provides real-time FWA detection prior to claim payment.
b. Provides pre-built analytic models to identify and analyze improper claims.
c. At a minimum, the solution shall provide the following tools;

- Predictive Analysis
- Link Analysis
- Surveillance and Utilization Review System

a. Capable of identifying and learning from fraudulent patterns and scenarios to reduce false positives and adapt predictive algorithms against emerging schemes.
b. Allows for new models for FWA detection as industry patterns are discovered.

6.3.3 EDITS

a. Allows for customized edits
b. Able to identify duplicate provider claims
c. Able to identify procedure bundling
d. Able to identify irregularities between coding combinations; procedure to diagnosis mismatches
e. Incorporates National Correct Coding Initiative (NCCI) data rules
f. Identifies Excluded Individuals and Entities (LEIE)
g. Identifies invalid or deactivated NPI numbers
h. Identifies charges significantly above or below geographic or national norms

6.3.4 RULES MANAGEMENT SYSTEM

a. Allows for customized payer specific reimbursement rules and policies

b. With Government-provided business rules, software shall be configured to ensure a minimum of 85% of claims transactions will be auto-adjudicated with straight-through processing, with no human touch points or human interaction.

6.3.5 ALERT SUMMARY REPORTING AND CASE MANAGEMENT DASHBOARD

a. Consists of a user-friendly, graphical user interface screen, to manage workloads and predefined work queues.
b. Provides alert reporting for flagged claims in zone and assigns ASR ID to individual claims.
c. Provides a role based display for total claims in zone and prioritizes claims that require assignment.
d. Provides role based capability to assign flagged claims to individual users.
e. Displays individual user workload assignments and allows for prioritizing claims.
f. Displays claim header and line level details.
g. Provides drill down capability for individual claims on a summary screen (Assigned User, ASR ID, Provider Name, Alert Rationale, FWA Model or Edit utilized).
h. Allow the user to link together ASRs that are being worked as part of the same case.
i. Accurately communicates the action to be taken on a flagged claim, provider, or group of providers (i.e., automatic denial, delay payment, investigate).
j. Provides all of the information necessary to take action (such as background data that may be required by an investigator to review an issue).
k. Provides GUI Map Interface icon associated with the ASR detail that will graphically display the geographic relationship between the provider and the beneficiary (when executed).
l. Allows for a provider profile features which contains defined metrics and attributes about the provider's patient population, billing activity, enrollment details, outputs, and summarized statistics.
m. Displays the description for displayed healthcare reference codes: i.e., Healthcare Common Procedure Coding System (HCPCS), Current Procedural Terminology (CPT), ICD-10, Place of Service (POS), Specialty Codes, and Berenson-Eggers Type of Service (BETOS) codes.
n. Allows form fields for users to record counts for the following:
    a. Actions they have taken; and
    b. Activities they have performed.
o. Provides a form for users to fill in additional information when specific rulings, actions, or activities are chosen.
p. Ensure users can access distinct recent Health Insurance Claim Number (HICN) claim examples to support evidence for the specific alert and applicable attribute(s) related and selected within the alert.

6.3.6 BUSINESS INTELLEGENCE REPORTING

a. Provide reporting views that are role-based to control access.
b. Display real time standard aggregate reports and display the results on the report.

c. Can monitor and track processor productivity, performance, and audits; and provide resulting metrics in ad hoc reports.
d. Allow the user to designate any chosen timeframe they want to display for all reports.
e. Allow the user to drill down to the supporting evidence from the aggregate reports.
f. Permit users to create ad-hoc reports and save them as user defined group reports making them accessible to other users within their organization.
g. Provide reports to users which illustrate the different model's performance.
h. Allow ad-hoc reporting capabilities that can drill down by Model or Edits, Geographic Region, Type of Service, Type of Provider, and other relevant variables defined by VA-FSC.
i. The system shall track the original source of alerts as well as the ultimate resolution of alerts and pass this information back to VA-FSC. The data collected shall provide for results reporting such as:
    - False Positive rates
    - Return on Investment and Cost Avoidance
    - Alerts and scoring results
    - Number of revocations, payment suspensions, claims denials, claims rejections or other actions.

6.3.7 QUERY, SEARCH AND EXPORT REQUIREMENTS

a. Provide the ability to query for alerts containing the chosen criteria:
    - ASR ID
    - Assigned User
    - Provider
    - Model or Edit Applied
b. Ability to search through user recorded notes and comments fields.
c. Ability search through all fields on the screen.
d. Ability export data from any FWA screen in the format of Excel, PDF or Word.

6.3.8 CAPACITY AND SCALABILITY

a. Capable of a capacity of 30 million claims annually. Claim volumes across lines of business may increase incrementally over the life of the contract.
b. Allows up to 5,000 active concurrent users, who may not be performing the same functions, on the software at the same time.
c. Can process up to 125,000 claims per day without performance degradation.
d. Allows response times on the user interface of no more than three seconds, regardless of the function being performed.
e. Supports adding IT infrastructure to scale up or scale out.
f. Can be configured to provide measurable throughput on end-to-end transaction processing, of less than three seconds.
g. The contractor shall complete capacity planning and review after each release.

6.3.9 SECURITY AND CONFIDENTIALITY

a. Architecture of the software provides safeguards for sensitive data within the VA Firewall; so patient and healthcare information confidentiality is maintained, and there is compliance within the regulatory environment, personally identifiable information (PII), Protected Health Information (PHI), and 38 U.S. Code §7332 Protected Data.

b. Supports Lightweight Directory Access Protocol (LDAP) integration for user access and authentication.

c. Supports single sign-on.

d. All system components shall be considered FISMA-High and shall comply with the following policies, handbooks, guidelines at the application and database levels:

   i. VA Handbook 6500 (Information Security Program) www.va.gov/vapubs/viewPublication.asp?Pub_ID=56

   ii. VHA Directive1906 (Data Quality Requirements for Healthcare Identity Management and Master Veteran Index) www.va.gov/vhapublications/ViewPublication.asp?pub_ID=2880

   iii. NIST 800-53 Version 4 (Security and Privacy Controls for Federal Information Systems and Organizations) www.csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

   iv. DISA-STIG (Defense Information Systems Agency Security Technical Implementation Guide) www.iase.disa.mil/stigs

   v. OMB M-04-04 (E-Authentication Guidance for Federal Agencies) www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

   vi. NIST 800-63-2 (Electronic Authentication Guideline) www.csrc.nist.gov/publications/drafts/800-63-2/sp800_63_2_draft.pdf

   vii. VA Handbook 0735-HSPD-12 (Homeland Security Presidential Directive 12 Handbook) www.va.gov/vapubs/viewPublication.asp?Pub_ID=758&FType=2

e. The Contractor shall identify the testing methods and tools used to verify compliance with the above security policies, handbooks, and guidelines.

f. The Contractor shall provide proof of compliance with all security policies, handbooks, and guidelines included in this document.

Deliverables:

A. Identification of Testing Methods and Tools used to Verify Compliance
B. Proof of Security Compliance

6.3.10 SYSTEM INTEGRATION AND INTEROPERABILITY

a. Capable of integrating with VA-FSC systems (such as Referral Authorization System (RAS), and Enrollment and Eligibility (EE)); in conjunction with the VA-FSC's adjudication of healthcare claims submitted by healthcare providers.

b. Consists of a system architecture that is open and provides interoperability capabilities through the use of web services using Simple Object Access Protocol (SOAP) or Representational State Transfer (REST).

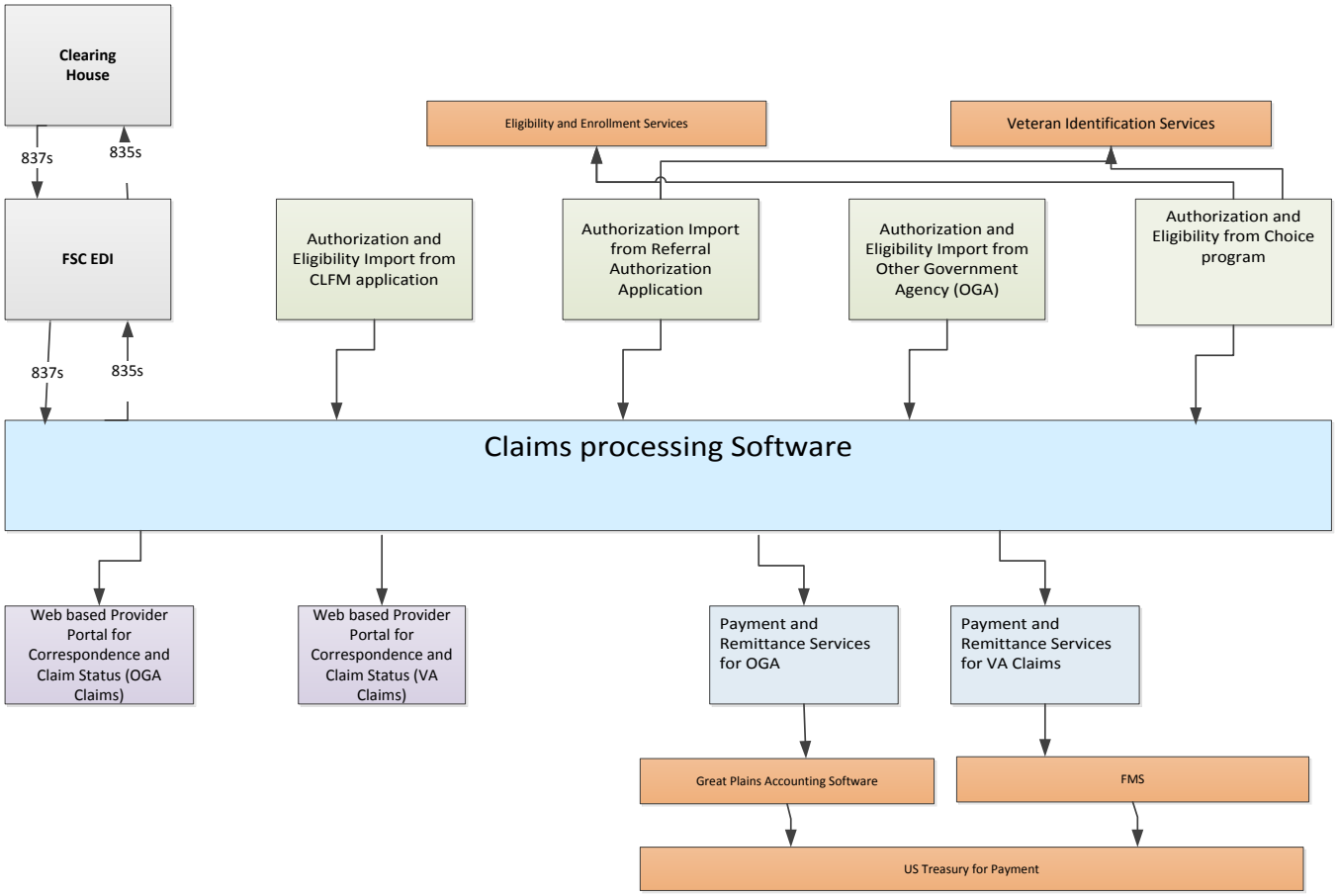
c. Integrates with Service Oriented Architecture (SOA) and Enterprise Service Bus (ESB) platforms.

d. Supports integration patterns approved by VA Enterprise Architecture, as well as Federal and NIST guidelines (HSPD-12 and Federal Identity, Credential, and Access Management (ICAM)).

e. Functional on all VA environments to include development, testing and production.

Exhibit 1A below depicts the current system interfaces.

Exhibit 1A



6.3.11 HIGH-AVAILABILITY

a. Supports a high availability configuration such as failover or clustering, and eliminates single points of failure.

6.3.12 TECHNICAL REFERENCE MODEL (TRM)

a. Contractor shall ensure all software and system components delivered under this contract can be approved on the VA Technical Reference Model (TRM), whose website can be found at https:// www.va.gov/trm.

b. Contractor shall submit a list of all software and system components to the VA-TRM group no later than 30 days following date of contract award for TRM approval.

c. Contractor shall ensure all software and system components are rated FISMA-HIGH in accordance with Section 2.0 FISMA requirements, which would increase the probability of software and components being TRM approved.

d. Contractor shall ensure all software and system components will be revised in accordance with TRM requirements.

e. Contractor shall ensure all software and system components are in compliance with VA TRM requirements within six (6) months of contract award, and stay in compliance with VA TRM from that point forward, as long as the software is in use by FSC.

Deliverable:

A. List of all software and system components no later than 30 days following date of contract award

6.3.13 TECHNOLOGY STACK

a. Shall be capable of running on the following technology stack components:

   a. Intel x64 hardware, using Windows 2012 R2 Operating System or Redhat Linux 7.x on a VMware virtualization platform. A technology stack is a set of software that provides the infrastructure for a computer. The stacks differ whether installed in a client or a server.

   b. Either Microsoft SQL Server 2012 R2, Microsoft SQL Server 2014 or Oracle 12c.

   c. SOAP, REST, JSON, or Oracle Service-Oriented Architecture and Oracle Service Bus, which will be the foundation for shared services.

b. Shall comply with VA's Technical Reference Model (TRM). Reference: www.va.gov/TRM.

6.3.14 HISTORICAL DATA PURGING AND RE-LOADING

a. Allows users to define data retention schedules, and can be programmed for automated archiving and purging data, based on age.

b. Able to perform both complete system data archival support and partial data archival support; based upon specified data criteria, such as dates.

c. Allows archival data to be restored by mid-level production support resources. Recovery tasks shall be performed without administrative rights to back end databases and other systems.

6.3.15 SYSTEM CONFIGURATION RETENTION AND MIGRATION

a. Able to back up and restore system configuration information and criteria, separate from claim data.

b. Capable of migrating system configurations between environments

6.3.16 DATA INPUT, CLAIMS INTAKE, AND DATA ACCESSIBILITY

a. Allows claim data input from various sources including EDI, Optical Character Recognition (OCR), and manual data entry.

b. Capable of displaying a rendered image of the claim from an electronic claim submission.

c. Can store hyperlinks to electronic documents or images in multiple ‘entities’ (such as member, claim, provider, and authorization) so this information can be viewed when clicked.

d. Can be easily navigated and cross-referenced, such that entities referenced in any object can be drilled down to a hyperlink that opens that entity without having to navigate back to the main screen.

e. Supports the following X12 5010 administrative transaction sets:

   i. 837I; 837P; 837D claim files

   ii. 835 payment files

   iii. 277CA and 999 response files

   iv. 270 eligibility inquiries

   v. 278 service reviews

   vi. 276 claim status inquiries

f. Allows update of the X12 and NCPDP administrative transaction sets to the next HIPAA mandated version.

7.0 FWA OPERATIONAL AND APPLICATION SUPPORT

The Contractor shall provide operational and application support for the FWA system that includes Defect Tracking and Resolution described in the following subsections.

7.1 DEFECT TRACKING AND RESOLUTION

The Contractor shall implement a quality management process that supports all scheduled and unscheduled maintenance, is coordinated with the VA-FSC, and ensures the proper identification, tracking, and timely resolution of defects in the operational FWA system. Defects shall be tracked in an approved defect tracking system with shared access by both the Contractor and VA-FSC. The Contractor shall propose its defect tracking system to VA-FSC for the agency's review and approval. The Contractor's quality management process shall ensure the identification, mitigation, and resolution of quality risks and production-level defects as early as possible in the development and production life cycles. The Contractor shall update VA-FSC on the status of all open defects and communicate the defect rate throughout the development and production life cycles.

Deliverable:

A. Defect Tracking System

7.2 END USER TRAINING

Training delivery methods may include webinars, in-person, and video teleconferencing sessions. The Contractor shall be prepared to accommodate ad hoc training delivery requests for VA-FSC-approved users and VA-FSC contractors. In-person training classes to facilitate initial user on-boarding shall take place at designated VA-FSC facilities. After receiving initial in-person training, participants may receive course updates through interactive delivery methods.

Prior to deployment of the operational FWA system, the Contractor shall:

- Develop a training plan that includes a plan for training identified trainers from each user organization.
- Develop training materials and a user guide for dissemination at all training sessions.
- Deliver demonstration and training sessions to different audiences, including VA-FSC and program integrity contractors, in both virtual and in-person environments. The Contractor's responsibilities for demonstration and training sessions include the following:
    - Any in-person sessions will be scheduled at the direction of at the VA-FSC furnished training facility.
    - The Contractor shall provide handouts of the presentation to the participants at in-person sessions.
    - For any virtual or in-person demonstration, the Contractor shall be prepared to walk through the FWA capabilities for participants using a real-time demonstration of system capabilities, and address user questions.

After the initial rollout of the FWA system to users, the Contractor shall offer ongoing support end-user training and self-help options as follows:

- The Contractor shall routinely create, update, and maintain technical support documentation related to incident prevention, error types, and resolution methods to assist users.

In addition to the regular training (regular training schedule is defined every month and every release) up to 10 additional ad hoc training sessions may be required.

Deliverable:

A. Training Plan
B. Training Materials
C. Training Sessions

8.0 GENERAL REQUIREMENTS

8.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall ensure COTS product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/EAOIT/OneVA/EAETA.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based

authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that

have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

8.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract.

8.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
	Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☐	☒	☐
5.2	☐	☒	☐
5.3	☐	☒	☐
5.4	☐	☒	☐
5.5	☐	☒	☐
5.6	☐	☒	☐
5.7	☐	☒	☐
5.8	☐	☒	☐
5.9	☐	☒	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

8.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.

b. The Contractor shall bear the expense of obtaining background investigations.

Within three (3) business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor

Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

c. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.

h. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints

The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).

d. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.

e. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) fingerprint results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior"; however the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

f. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.

Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

All Contractor and subcontract personnel must read and abide by the security requirements in place at this facility. Failure to comply with these security requirements may result in revocation of physical and/or electronic access privileges and/or termination of the contract for default.

The Contractor shall not use any offshore resources (i.e. personnel, hardware, and software) in support of the services being provided under this contract. For the purposes of this contract, offshore is defined as being any location outside the United States, its possessions, and Puerto Rico.

Failure to complete the work in a timely manner, or by any required completion date, caused by delays in requesting security clearances, or due to revocation of access privileges resulting solely from the actions of the Contractor or their personnel, is not sufficient reason to warrant an extension in contract time or cost.

Deliverable:

A. Contractor Staff Roster

8.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

8.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

Performance Objective	Performance Standard	Acceptable Performance Levels

Performance Objective	Performance Standard	Acceptable Performance Levels
A. Technical Needs	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Offers quality services/products 5. Provides configurable software and perpetual license 6. Provides software maintenance and technical support	Satisfactory or higher Software product meets all capability, functionality, and technical requirements set forth herein. Contractor records all technical services performed and delivers Technical Services Report on time each month.
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in timely manner 3. Notifies customer in advance of potential problems 4. Provides software updates and upgrades	Satisfactory or higher Contractor keeps COR informed of actions Contractor informs COR of updates and upgrades no later than 5 workdays after they become available. Contractor and IT team coordinate update and upgrade of software.
C. Project Staffing	1. Currency of expertise 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	1. Provided valuable service to Government 2. Services/products delivered were of desired quality and in accordance with contractual requirements.	Satisfactory or higher Deliverables are provided to VA-FSC no later than when they are required, in accordance with the schedule contained herein. If Contractor believes a deliverable will be late; Contractor tells COR, by email and phone including why deliverable will be late and when it will be delivered. Contractor does this at least 2 business days prior to the

Performance Objective	Performance Standard	Acceptable Performance Levels
		due date.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

8.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when authorized contract staff work at a Government location as required, in order to accomplish the tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, **CONSOLIDATED** and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

The VA Financial Services Center (FSC) is a high security government facility. For purposes of this specification section, “FSC,” “premises”, “site,” “Center,” and “facility” shall mean the FSC building and surrounding property, including parking areas.

Access into the FSC is only allowed through the main entrance. The loading dock may be used to load and unload materials only (not access in and out of the FSC), and only during the hours it is open (Monday – Friday, 8:00 AM to 4:00 PM, excluding official Government holidays). If the Contractor desires to open any normally closed secure doors (or make an opening into the building structure), then it is the Contractor’s responsibility to request additional armed security officer services (using a form provided by the FSC’s Physical Security Officer) to guard the door and control access, allowing entry only by authorized Contractor and government personnel (though the services are paid for by the Contractor, the security officers remain under the direction of the FSC’s Physical Security Officer). All personnel entering through this normally closed opening shall be screened by the security officer using a handheld metal detector. All items will be manually inspected (this includes opening and inspecting all packages) prior to being allowed entry. Additional security officer services shall be requested at least 48 hours in advance of when a security officer is needed. Such services shall be provided only by the FSC’s approved armed security officer services provider. The Contractor shall reimburse the FSC’s armed security officer services provider within 30 days of receipt of the invoice for such services. Billable rates for the additional armed guard services shall be at the same rates charged to the government (approximately $40/hour, with a 4 hour minimum per security officer, and at least 48 hours' notice of any cancellation to avoid being billed for the scheduled services). A valid credit card number and type, along with the name on the card and the expiration date, must be provided before the security officer services will be scheduled. Should the Contractor fail to reimburse the FSC’s armed security officer services provider as specified above, the FSC shall reimburse the security officer services provider directly and deduct such costs from this contract, plus a 2 percent administrative fee. Other security methods proposed by the Contractor (such as temporary walls) may be reviewed and approved, modified, or disapproved by FSC. The determination as to whether or not what the Contractor proposes meets the necessary level of security shall be determined by the FSC’s Chief, Security Services.

Each person requiring unescorted physical access to the property will be required to submit personal identifying information (full legal name (first, middle, and last), date of birth, state issued driver’s license or identification card number and the state that issued it, and name as it appears on the identification card. This information will be used to perform a criminal history check. Visitors who are not subjected to the criminal history check must be escorted at all times by someone who has been issued a permanent FSC ID badge. The cost of conducting the criminal history check is the responsibility of the FSC. The cost, if any, of arranging for an escort is the responsibility of the Contractor. The Contractor shall pre-screen all personnel requiring physical access to the property to ensure they are legally able to work in the U.S. and not currently sought by law enforcement authorities. Adjudication of information discovered during or after the criminal history check is solely the responsibility of the Chief, Security Services.

Being admitted entry into the FSC based on a finding of no criminal history does not convey any security clearance. The Chief of Security Services may revoke physical access privileges at any time if criminal history is discovered, or if the person commits security incidents warranting such revocation.

NOTE: Personnel doing work on the FSC site under contract to GSA will also be required to submit additional documentation, be fingerprinted, and be determined by the Department of Homeland Security (DHS) Federal Protective Service (FPS) to be suitable to work on this property.

8.6 GOVERNMENT FURNISHED PROPERTY

Not applicable

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

i. Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

j. VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A1.1. VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's

work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

k. **Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)**

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

A1.2. Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards and http://www.section508.gov/content/learn/standards. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products
- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self-contained, closed products
- ☐ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

A1.3. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A1.4. Compatibility with Assistive Technology

The Section 508 standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device. Section 508 requires that the EIT be compatible with such software and devices so that EIT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

A1.5. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

Deliverable:

A. Final Section 508 Compliance Test Results

l. Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.

5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

m. **Confidentiality and Non-Disclosure**

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used

for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

n. INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold

payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or a Memorandum of Understanding-Interconnection Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not Applicable

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

Not Applicable

B6. SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or

integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

Not Applicable

B9. TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

2) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access *[to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

ADDENDUM C – VAAR- 852.273-75 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

The Contractor and their personnel shall be subject to the same Federal laws, regulations, standards and VA policies as VA personnel, regarding information and information software security. These include, but are not limited to Federal Information Security Management Act (FISMA), Appendix III of OMB Circular A-130, and guidance and standards, available from the Department of Commerce's National Institute of Standards and Technology (NIST). This also includes the use of common security configurations available from NIST's Web site at http://checklists.nist.gov.

To ensure that appropriate security controls are in place, Contractors must follow the procedures set forth in "VA Information and Information Software Security/Privacy Requirements for IT Contracts" located at the following Web site: http://www.iprm.oit.va.gov.

ACCESS TO VA INFORMATION AND VA INFORMATION SOFTWARE

All Contractor employees shall comply with the same standards, conditions and restrictions placed on VA personnel for the handling of VA sensitive data; to include the standards, conditions, and restrictions contained in VA Directive and Handbook 6500. www.va.gov/vapubs/viewPublication.asp?Pub_ID=56

In accordance with VA Directive/Handbook 0710, each position performed under a contract that requires access to a VA information software must have the designated position sensitivity level (High, Moderate, or Low Risk) and associated background investigation requirements (Background Investigation (BI), Minimum Background Investigation (MBI), or National Agency Check with written Inquiries (NACI), respectively) documented in the contract. Each person performing in such a position must complete and submit certain forms/documents (as required by the VA Security Investigation Center (SIC) and be fingerprinted by VA Human Resources staff (at no cost to the Contractor). The forms may be downloaded from the SIC website, or provided by the Contracting Officer (CO) after receiving the names and Social Security Numbers for all personnel (this information will be submitted to the SIC by the CO, along with billing information). The forms must be completed and submitted to the CO. It is incumbent upon the Contractor to ensure the forms are submitted timely to avoid delays, as the CO must submit these documents to SIC before access to VA computer software or access to the FSC facility is authorized. For Moderate and High Risk positions, access cannot be granted until the Contractor employee has been issued the applicable VA security clearance.

NOTE: False statements on the personal history form or fingerprint cards are punishable by law and could result in fines of up to $2,000 and imprisonment for up to 5 years. Contractor shall request access to VA information and VA information software for employees, subcontractors and affiliates only to the extent necessary: (1) to perform the services specified in the contract; (2) to perform necessary maintenance functions for electronic storage or transmission media necessary for performance of the contract, and (3) for individuals who first satisfy the same conditions, requirements and restrictions that comparable VA employees must meet in order to have access to the same type of VA information. These restrictions include the same level of investigative requirements, as applicable, with the following exceptions:

Contract personnel not accessing VA information resources such as personnel hired to maintain the facility grounds, construction contracts, utility software Contractors, etc.

Contract personnel with limited and intermittent access to equipment connected to facility networks where no Protected Health Information (PHI) is available, including Contractors who install, maintain and repair networked building equipment such as fire alarm; heating, ventilation and air conditioning equipment; elevator control software, etc.

All Contractors and subcontractors working with sensitive VA information are subject to the same investigative requirements as those of regular VA appointees or employees who have access to the same type of information. The level of background security investigation will be in accordance with VA Directive 0710 and Handbook 0710, available at http://www1.va.gov/vapubs/.

The position risk and sensitivity level(s) for this effort have been designated at as ***Medium*** Risk. Position Sensitivity and Background Investigation: The position sensitivity and level of background investigation commensurate with the required level of access is:

- ☐ Low/NACI
- ☒ Moderate/MBI
- ☐ High/BI

The Contractor shall satisfy all requirements for appropriate security eligibility in dealing with access to sensitive information and information software belonging to or being used on behalf of the Department of Veterans Affairs (VA). To satisfy the requirements of the VA; a Minimum Background Investigation (MBI) or National Agency Check and Inquiries (NACI), based on position level shall be conducted prior to performing work under this contract. Appropriate Background Investigation (BI) forms will be provided upon award of contract, and are to be completed and returned to the VA FSC Personal Identification Verification (PIV) Sponsor for processing and submission to VA Security Investigation Center (SIC). The PIV process currently takes approximately 3 4 weeks for completion. All BI forms shall be submitted to the VA FSC PIV Sponsor within 5 days after contract award. Contractors will be notified by the VA Office of Security and Law Enforcement (OSL&E) when the BI has been completed and adjudicated.

All costs associated with obtaining clearances for Contractor provided personnel will be the responsibility of the Contractor. Further, the Contractor will be responsible for the actions of all individuals provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor will be responsible for all resources necessary to remedy the incident.

All Contract personnel and subcontract personnel requiring access to VA information and VA information software shall do the following before being granted access to VA networks:

Sign a Non-Disclosure Agreement to acknowledge understanding of and responsibilities for compliance with the National Rules of Behavior, relating to access to VA information software and proprietary information;

Successfully complete VA Information Security Awareness training, and annual refresher training;

Successfully complete VA General and HIPAA Privacy training, and annual refresher training; and

Successfully complete all additional security and/or privacy training as VA personnel with equivalent information software access, as required, particularly as determined relevant to the contract employee's position.

All Contractor employees must sign all required forms and paperwork and complete all required courses within one week of commencing work in accordance with this contract. These requirements must be met before access will be granted to software and prior to badge issuance. Certain training is also required to be completed annually, in accordance with VA-FSC policy. The courses must be taken at the FSC facility or another VA location as directed by the COR. Failure to complete this mandatory training within the required timeframe will be grounds for suspension or termination of all physical and electronic access privileges and removal from work on the contract until such time as the training is completed. Removal from work on the contract due to failure to complete mandatory training shall result in a reduction in overall contract cost, and is not sufficient reason to warrant an extension in contract time or cost.

For information software which is hosted, operated, maintained or used on behalf of VA at non VA facilities, Contractors are fully responsible and accountable for ensuring compliance with all FISMA, NIST, FIPS, and VA security policies and procedures. The Contractor security control procedures must be identical, not equivalent, to those procedures used to secure VA software. A privacy impact assessment (PIA) must also be included and approved by VA Privacy Service prior to operational approval. All external Internet connections involving VA information must be reviewed and approved by VA prior to implementation.

The security controls must be in place prior to hosting, operation, maintenance, or use of the information software, or software by or on behalf of VA. Security controls for collecting, processing, transmitting, and storing of personally identifiable information (PII) must be in place prior to operating.

Outsourcing (Contractor facility/Contractor equipment/Contractor staff) of software or network operations, telecommunications services, or other managed services requires certification and accreditation of the Contractor’s software prior to operation of the software. Government owned (government facility/government equipment), Contractor operated software require a software interconnection agreement for all software connected to VA networks.

The Contractor must adhere to all FISMA, FIPS and NIST legislation and standards related to conduct of an annual security controls assessment and review and updates to the Privacy Impact Assessment (PIA). Any deficiencies noted during this assessment must be provided to the VA Contracting Officer and the Information Security Officer

(ISO) for entry into VA's Plan of Action and Milestone (POA&M) management process. The Contractor will use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor procedures will be subject to periodic, unannounced assessments by VA officials. The physical security aspects associated with Contractor activities will also be subject to such assessments.

All electronic storage media used on non-VA leased or owned IT equipment that is used to store, process, or access VA sensitive information must have all VA sensitive information removed, cleared, sanitized, or destroyed in accordance with VA policies and procedures upon the earlier of: (1) completion or termination of the contract or (2) disposal or return of the IT equipment by the Contractor or any person acting on behalf of the Contractor.

As a consequence of this agreement, the Contractor may become a temporary custodian of VA data on behalf of VA. Information made available to the Contractor by VA for the performance or administration of this contract shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. This clause expressly limits the Contractor's rights to use data as described in Rights in Data – General, FAR 52.227 14 (d) (1).

Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor will refer all requests for, demands for production of, or inquiries about, VA information and information software to the VA Contracting Officer for response.

The Contractor shall not release information protected by either 38 USC 5705 or 7332 in response to a court order, and shall immediately refer such court orders to the Contracting Officer for response.

VA information will not be co-mingled with any other data on the Contractor's or subcontractors' information software or media storage software in order to ensure VA requirements related to media sanitization can be met. VA reserves the right to conduct onsite inspection of information destruction or media sanitization procedures to ensure they are in compliance with VA policy requirements.

The VA data associated with this contract has been categorized from VA sensitive to VA critical.

As custodian on behalf of VA, the Contractor shall store, transport and transmit VA data, or any derivatives thereof, utilizing a FIPS 140 2 validated encryption module.

Prior to contract termination, Contractor will not destroy VA information received from VA or gathered or created by Contractor in the course of performing this contract without prior written approval by the VA Contracting Officer.

At contract termination or upon demand, the Contractor shall return all VA data, and derivatives thereof, and shall purge or destroy all electronic, magnetic, optical or hardcopy media in accordance with VA media sanitization procedures.

Contractor will receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of this contract and applicable federal and VA information confidentiality and security laws, regulations and policies. Applicable federal information security regulations include all Federal Information Processing Standards (FIPS) and Special Publications (SP) issued by the National Institute of Standards and Technology (NIST). If federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information software after execution of the contract, or if NIST issues or updates applicable FIPS after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies, including FIPS or SP, in this contract.

The Contractor shall not make copies of VA information except as necessary to perform this agreement or to preserve electronic information stored on Contractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor needs to be restored to an operating state.

A determination by VA that the Contractor has violated any of the information confidentiality and security provisions of this contract shall be sufficient grounds for VA to terminate the contract for default.

SECURITY INCIDENT INVESTIGATION

The term “security incident” means an event that has or could have resulted in loss of or damage to VA assets and/or sensitive information; or an action that breaches VA security procedures. Within one (1) hour of a security incident, the Contractor shall simultaneously notify the COR, the VA Network Security Operations Center (vansoc@va.gov), and the designated ISO/Privacy Officer for the contract of any known or suspected security/privacy incident, or any unauthorized disclosure of sensitive information, including that contained in software(s) to which the Contractor has access.

To the extent known by the Contractor, the Contractor’s notice to VA will identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where VA information/assets were placed at risk or compromised), and any other information that the Contractor considers relevant.

Contractor will simultaneously report the incident to the appropriate law enforcement entity or entities of jurisdiction in instances of theft or break in. The Contractor, its

employees, and its subcontractors and their employees will cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor will cooperate with VA in any civil litigation to recover VA information, to obtain monetary or other compensation from a third party for damages arising from any incident, or to obtain injunctive relief against any third party arising from, or related to, the incident.

To the extent practicable, Contractor shall mitigate any harmful effects on individuals whose VA information was accessed or disclosed in a security incident. In the event of a data breach with respect to any sensitive personal information processed or maintained by the Contractor or subcontractor under the contract, the Contractor is responsible for liquidated damages to be paid to VA and remediation to potentially harmed individuals (such as offering and paying for credit monitoring).

SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the VA Office of Inspector General, reserves the right to evaluate any or all of the security controls implemented by the Contractor under the clauses contained within the contract. With ten (10) working days' notice, at the request of the Government, the Contractor will fully cooperate and assist in a Government sponsored security controls assessment at each location where VA information is processed or stored; or where information software are developed, operated, maintained, or used on behalf of VA; including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments), as determined by VA, in the event of a security incident or at any other time.